

Remote Access is a...

- **Gateway to NIH data and resources**, providing flexibility and increased efficiency to users who work off-site (e.g., traveling, at home and wireless users).
- **Privilege** granted when management has determined you have a job-related need for remote access to the NIHnet. Your privilege can be revoked if you fail to comply with the terms of the *Remote Access User Certification Agreement*. All remote users must sign this agreement.
- **Security Issue** because inadequate safeguards can lead to unacceptable risks, e.g., network outage, malicious theft or modification of data and invalidated research.

NIH Secures Remote Access by:

- 1) **Policy, Standards and Procedures:** These documents are listed under *Useful Resource Web Sites*. The requirements are mandatory and apply to all employees, contractors, and other authorized users.
- 2) **Restricting Access Methodology:** Access to NIHnet must be routed through secure services approved by the NIH Chief Information officer (CIO). Approved services include:
 - **Virtual Private Network (VPN):** Home or office users with broadband (high-speed) connections; users with commercial dialup providers or Integrated Services Digital Network (ISDN) lines; users of commercial wireless services or temporary broadband connections; or users in remote telework centers or co-located in non-NIH space. NIH provides a VPN client that ensures connections have strong authentication and encryption. Such protection includes intrusion detection systems, firewalls, and anti-virus software.

- **PARACHUTE:** Official dialup service managed by CIT, ideal for staff and contractors with analog or ISDN dialup capability. Allows logon to NIHnet using a modem and standard telephone or ISDN line.
- **Alternate Remote Access:** Institute or Center (IC) submits a request through Information System Security Officer (ISSO) to NIH Incident Response Team (IRT). Only the NIH CIO approves these exceptions.

3) Requiring Encryption for VPN Service:

All access must be accomplished directly between end user systems and NIH secure remote access gateways. Encryption must be based on the Advanced Encryption Standard ((AES) or the Triple Data Encryption Standard (3DES) in accordance with Federal Information Processing Standard (FIPS)-197. Wireless devices must also use Wired Equivalent Privacy (WEP) encryption.

4) Requiring Host Modem Registration with NIH and Approval by NIH CIO:

Unauthorized modems are prohibited. Host modems are modems connected to any NIH-connected network or equipment that can receive calls from the outside. Modems are authorized if they are part of PARACHUTE, approved for maintenance purposes, connected to fax machines/copiers with a network connection or otherwise approved by the NIH CIO. Authorized modems must be disconnected when not in use, have auto-answer disabled, disabled for outbound dialing except for authorized connections, and include strong authentication with non-default passwords, tokens, or one-time password use.

10 Rules to Help Users Ensure Secure Remote Access

Rule 1: Keep your anti-virus software up-to-date. Without current anti-virus software, your computer can be infected with a virus that can quickly spread to other systems connected to NIHnet. Anti-virus software can be downloaded from <http://antivirus.nih.gov> to government and personally owned computers that access the

NIHnet.. Easy to follow directions for Windows machines can be found at:

<http://irm.cit.nih.gov/security/how-to.pdf/>.

Automatic updates at least every two weeks are recommended to help protect against the spread of virus and worm infections. Contact your ISSO or the NIH Help Desk if you need assistance.

Rule 2: Configure privately-owned computers to be secure and keep private and government-owned computers current with patches.

Computers generally arrive (out of the box) with most services turned on, making them vulnerable to hacker exploits. Use the NIH configurations checklists as guidance (<http://www.cit.nih.gov/security-securing.asp>). Check for patch updates periodically at <http://windowsupdate.microsoft.com> for Windows systems. Consider a personal firewall for computers connected to the Internet for extended periods, e.g., cable.

Rule 3: Use, maintain and store highly sensitive information on NIHnet servers when feasible. Avoid storing sensitive information on laptop computers when possible. Know the sensitivity of the information you access or transmit and apply appropriate safeguards, including encrypted transmission, if appropriate.

Rule 4: Complete the NIH Computer Security Awareness Course at <http://irtsectraining.nih.gov/>.

Rule 5: Use only authorized, licensed NIH software on government-owned systems and do not alter the configuration of such systems unless authorized. This includes software on the NIH desktop Information Systems Designated Procurement (ISDP) web site at <http://isdpcit.nih.gov/> or other software approved by your IC management.

Rule 6: Secure your computer work environment. Consider who has access to your work area (telecommunication center, home, airport, hotel, etc.). Ensure there is no unauthorized access. Be wary of the possibility

of theft—especially in public areas. Consider installing a password-protected screen saver.

Rule 7: Create Strong Passwords. Never use default passwords—change them immediately. Comply with the NIH Password Policy at http://irm.cit.nih.gov/nihsecurity/pwd_policy.doc and review the NIH User Password Requirements at http://irm.cit.nih.gov/nihsecurity/pwd_requirements.doc. Never “save” passwords in a login script or share them with other users.

Rule 8: Judiciously apply the Limited Authorized Personal Use Policy Review the definition of limited personal use at: (<http://www1.od.nih.gov/oma/manualchapters/management/2806>). Don’t use non-NIH e-mail accounts or other external resources to conduct NIH business to avoid confusing personal and official business.

Rule 9: Exercise caution before you download programs onto your computer. Some website downloads contain malicious code, including spyware. Consider running *Ad-Aware* from <http://antivirus.nih.gov/> to remove spyware type programs that may inadvertently be loaded on your desktop. Free shareware may be sharing viruses with other computers—that could infect NIHnet.

Rule 10: Follow the NIH Backup Guidance http://irm.cit.nih.gov/security/sec_policy.html. Backup critical or important information regularly and often.

Useful Resource Web Sites:

Remote Access Links

- NIH Remote Access Web site: <http://remoteaccess.nih.gov>.
- NIH Remote Access Policy http://irm.cit.nih.gov/nihsecurity/NIH_RAS_Pol.pdf
- Remote Access Security Standards and Procedures http://irm.cit.nih.gov/nihsecurity/NIH_RAS_Sec_Stand_Proc.pdf

- NIH Wireless Network Policy <http://www3.od.nih.gov/oma/manualchapter/s/management/2807> and the NIH Wireless Security Policy http://irm.cit.nih.gov/security/sec_policy.html
- User Certification Agreement http://irm.cit.nih.gov/security/RA_User_Cert_Agreemt.pdf

General Security Links

- Information Security Home Web Page: <http://www.cit.nih.gov/security.html>
- NIH IT General Rules of Behavior: <http://irm.cit.nih.gov/security/nihitrob.html>
- Practical Computer Security Advice for Users: http://securitynews.nih.gov/security_advice.html
- Guidance for Securing Data on Portable Systems: <http://irm.cit.nih.gov/security/GuixSecuData.html>
- Telework Rules: <http://www.telework.gov/>

Need Help and Advice?

NIH Help Desk: 301-496-HELP (4357) or send a message to helpdesk@nih.gov. Support is available M-F from 7:00 a.m. till 6:00 p.m., EST, for technical and security problems. After hours support is available for system outages or security incident emergencies only.

IC Information System Security Officers can help with computer policy, issues, or problems. Report suspected computer security incidents to your ISSO. The roster is located at: <http://irm.cit.nih.gov/nihsecurity/scroster.html>

Examples of **computer incidents** include: hacker attacks, suspected fraud, waste, or abuse of a system, inappropriate use, improper disclosure of sensitive information, inability to access files, and theft of data.

IC ISSO _____

Phone: _____

Remote Access

Secure Connections to the NIH Network (NIHnet)



**Information Security and Awareness Office
Office of the Deputy Chief Information Officer
Center for Information Technology
National Institutes of Health**

September 2003

